02P11863

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 06 062 A 1**

(51) Int. Cl.[7]: **H 04 L 9/00**
G 06 F 12/14

(21) Aktenzeichen: 100 06 062.5
(22) Anmeldetag: 10. 2. 2000
(43) Offenlegungstag: 30. 8. 2001

(71) Anmelder:
Excelsis Informationssysteme GmbH, 70178 Stuttgart, DE

(74) Vertreter:
Patentanwälte Böck + Tappe Kollegen, 97074 Würzburg

(72) Erfinder:
Ollhäuser, Marc, 70329 Stuttgart, DE

(56) Entgegenhaltungen:

DE	195 40 973 C2
DE	41 26 760 A1
US	58 64 683
US	58 12 671
US	57 37 422
US	54 06 624
JP	11-3 53 280 A

SPIELVOGEL, J.: Datenschutz durch Datenverschlüsselung, in: Sonderdruck aus Nachrichtentechnische Zeitschrift, Bd. 29 (1976) 6, S. 439-440;
Prospekt "SecuriCrypto", 1989;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Tastaturschlüssel

(57) Die Erfindung betrifft ein Verfahren und eine Einrichtung zur gesicherten Verarbeitung und/oder Übertragung von digitalen Daten, insbesondere bei vernetzten Computersystemen, wobei in zumindest ein Computersystem eingehende Daten vor der Weiterbenutzung innerhalb des Computersystems einem kryptographischen Verfahren unterzogen werden.

DE 100 06 062 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zur gesicherten Verarbeitung beziehungsweise Übertragung digitaler Daten, insbesondere zur Übertragung vertraulicher Daten in vernetzten Computersystemen. Weiterhin betrifft die Erfindung eine Einrichtung zur vorteilhaften Durchführung des erfindungsgemäßen Verfahrens.

In vielen Bereichen des täglichen Lebens wird heutzutage der Austausch digitaler Daten über vernetzte Computersysteme betrieben. Inzwischen gewinnt auch der Zahlungsverkehr unter Benutzung offener Computernetze, wie beispielsweise dem Internet, zunehmend an Bedeutung. Da die Datenströme, insbesondere in offenen Netzen wie dem Internet, abgehört werden können, entsteht das Problem, vertrauliche Daten bei der Übermittlung vor unbefugtem Einblick zu schützen, also die Vertraulichkeit der übertragenen Daten herzustellen.

Weiterhin muß die Herkunft der Daten, also die Authentizität, gesichert sein und schließlich müssen die Daten vor Manipulation geschützt sein, also deren Integrität gesichert sein.

Zur Lösung dieses Problems ist eine große Anzahl an Verfahren bekannt, mit denen die Vertraulichkeit, Integrität bzw. Authentizität der übertragenen Daten gewährleistet werden kann. Hier sind beispielsweise der sog. Kerberos®-Authentifikationsdienst, das symmetrische Data-Encryption-Standard-Verfahren (DES®) und dessen Abwandlungen oder auch die asymmetrischen Standard-Public-Key-Verfahren, wie zum Beispiel RSA® oder Diffie-Hellmann, zu nennen.

Diese bekannten Verfahren wurden bisher jedoch nur für die Datenübertragung zwischen den einzelnen Computersystemen eines Computernetzwerks angewendet. Damit kann zwar eine gesicherte Datenübertragung auf dem Computernetz selbst gewährleistet werden, ein Angriff auf vertrauliche Daten, insbesondere durch auf dem Rechner vorhandene, unbefugt auf die vertraulichen Daten zugreifende Programme wie Viren oder sog. Trojanische Pferde ist innerhalb des einzelnen Computersystems jedoch nach wie vor möglich. Die auf diese Weise unbefugt gewonnenen Daten können anschließend, evtl. auch zu einem späteren Zeitpunkt, über das Netz verschickt und so zentral gesammelt und ausgewertet werden.

Um das Abfragen einer Tastatureingabe, insbesondere eines über die Tastatur eingegebenen Paßworts durch unbefugte Viren oder Trojanische Pferde auszuschließen wird vereinzelt eine Paßworteingabe mittels Mausbewegungen über eine am Bildschirm dargestellte Tastatur durchgeführt. Jedoch besteht auch hier das Problem, daß die Mausbewegungen durch unbefugte Mittel abgefragt werden können.

Aufgabe der Erfindung ist es deshalb, ein Verfahren sowie eine vorteilhafte Einrichtung zur Durchführung des Verfahrens vorzuschlagen, die die Sicherheit sensitiver Daten, insbesondere deren Vertraulichkeit und Integrität, auch innerhalb des Computersystems gewährleisten.

Die Aufgabe wird dadurch gelöst, daß die in das Computersystem eingehenden Daten vor der Weiterbenutzung, also beispielweise Weiterverarbeitung in einem Programm, Zwischenspeicherung im Arbeitsspeicher oder Weiterleiten an ein anderes Computersystem, einem kryptographischen Verfahren unterzogen werden, so daß die Daten innerhalb des bzw. der Computersysteme in kryptographisch verschlüsselter Form vorliegen. Dabei ist es vorteilhaft das kryptographische Verfahren möglichst frühzeitig auf die eingehenden Daten anzuwenden. Es ist unerheblich, ob die Verschlüsselung in einer externen Komponente, einer internen Komponente, betriebssystemseitig, beispielsweise durch Anpassung der Gerätetreiber (also der Umsetzung eines komponentenspezifischen Formats in ein standardisiertes Format einer Computereinheit) oder unmittelbar danach, programmtechnisch, schaltungstechnisch oder als Kombination daraus, erfolgt. Vorteilhaft bei einer betriebssystemseitigen Anwendung des Verschlüsselungsverfahrens ist, daß bereits vorhandene Komponenten (die Hardware) weiter verwendet werden können. Zu bedenken ist dabei ferner, daß um so mehr gerätespezifische Eigenheiten berücksichtigt werden müssen, je früher und damit je näher an der Komponente das Verschlüsselungsverfahren angewendet wird, so daß es unter Umständen sinnvoll sein kann, die Verschlüsselung der ankommenden Daten erst zu einem späteren Zeitpunkt, beispielsweise erst im Anschluß an den Gerätetreiber, vorzunehmen. In jedem Fall wird der unbefugte Zugriff auf sicherheitsrelevante Daten, beispielsweise durch Viren oder Trojanische Pferde, dadurch erschwert, daß die Daten innerhalb des Computersystems nur noch in kryptographisch verschlüsselter Form vorliegen und in dieser Form weiterverarbeitet, zwischengespeichert bzw. übertragen werden. Je nach Erfordernis können aus dem Computersystem hinausgehende Daten, vorab einem inversen kryptographischen Verfahren unterzogen werden.

Als besonders vorteilhaft erweist es sich, wenn das kryptographische Verfahren von einem Verschlüsselungsclient auf die von einer Device her eingehenden Daten angewendet wird. Als Device sind, wie in der Computertechnik üblich, alle eigenständigen Einheiten, die mit dem Computersystem zusammenarbeiten, zu verstehen. Dieser Begriff umfaßt beispielsweise externe und interne Geräte wie Tastaturen, Laufwerke, Modems, Massenspeicher, Netzwerkarten und andere Einheiten. Durch die Anwendung des kryptographischen Verfahrens auf die von einer Device her eingehenden Daten liegen alle von den jeweiligen eigenständigen Einheiten stammenden Daten innerhalb des Rechners nur in verschlüsselter Form vor, so daß ein Angriff entsprechend erschwert wird. Ist eine bidirektionale Kommunikation mit der Device erforderlich können zumindest die Steuersignale, aber auch die sonstigen Daten, je nach Erfordernis, vor dem Versand durch den Verschlüsselungsclient zunächst einem inversen kryptographischen Verfahren unterzogen werden. Wie bereits ausgeführt, kann die Verschlüsselung oder auch die Entschlüsselung bereits in der Eingabeeinrichtung oder aber auch betriebssystemseitig erfolgen. Der Verschlüsselungsclient kann dabei beliebig schaltungstechnisch, programmtechnisch oder auch als eine Kombination, beispielweise als Programm das auf Funktionen eines kryptographischen Co-Prozessors zugreift, realisiert sein.

Als besonders vorteilhaft erweist es sich, wenn die von einer Eingabeeinrichtung, insbesondere die von einer Tastatureinrichtung stammenden Daten erfindungsgemäß einem kryptographischen Verfahren unterzögen werden. Unter Eingabeeinrichtung sind dabei beliebige, Anwendereingaben aufnehmende Systeme zu verstehen, wie beispielsweise Touchscreens, Computermäuse, Fingerabdruckscanner, Kartenlesegeräte oder ähnliches. Über alle diese Geräte werden sicherheitsrelevante Daten, beispielsweise Zugangscodes, Paßwörter, Fingerabdrücke und ähnliches eingegeben, die mittels des erfindungsgemäßen Verfahrens vor Angriffen geschützt werden können. Als Tastatureinrichtung sind nicht nur Tastaturen an sich, sondern auch, wie bei modernen Computertastaturen in zunehmenden Maße üblich, integrierte Geräte mit Touchpads, Kartenlesegeräte und dergleichen, zu verstehen. Gerade über die Tastatur werden häufig sicherheitsrelevante Daten, beispielsweise in Form von Paßwörtern eingegeben, so daß hier Schutzmaßnahmen gegen Angriffe besonders vorteilhaft sind.

Vorteilhafterweise werden die dem kryptographischen

Verfahren unterzogenen Daten von einem authorisierten, als Gateway bezeichneten Mittel empfangen und von diesem einem inversen kryptographischen Verfahren unterzogen, so daß die Daten wieder in ihrer Ursprungsform vorliegen. Dieses Gateway kann je nach Erfordernis beim ursprünglichen, ersten Computersystem, an dem die Daten eingehen, vorgesehen sein, oder auch bei einem zweiten, räumlich davon getrennten Computersystem vorgesehen sein oder eventuell auch auf beiden Computersystemen vorhanden sein. Das Gateway kann dabei, wie auch der Verschlüsselungsclient, programmtechnisch, schaltungstechnisch oder als Kombination aus beiden realisiert sein. In jedem Fall liegen die durch das Gateway entschlüsselten Daten wieder in ihrer ursprünglichen Form vor, so daß die Daten weiterverarbeitet werden können, und somit beispielsweise die Zugangsberechtigung des Benutzers feststellt werden kann und diesem der Zugang zum System oder bestimmten Systemfunktionen gestattet wird. Auch können die entschlüsselten Daten an andere berechtigte Anwendungen weitergegeben werden.

Es erweist sich als besonders vorteilhaft, wenn die Daten vor der Übertragung zu einem zweiten Computersystem von einem zusätzlichen Verschlüsselungsmittel einem weiteren kryptographischen Verfahren unterzogen werden. Dabei ist es unerheblich, ob die Daten in verschlüsselter Form oder in ihrer ursprünglichen Form, nachdem sie von einem Gateway des ersten Computersystems einem inversen kryptographischen Verfahren unterzogen wurden, vorliegen. Bei dieser erneuten kryptographischen Verschlüsselung kann das ursprüngliche oder auch ein anderes kryptographisches Verfahren verwendet werden. Ebenso kann ein anderer, neuer Schlüssel zur kryptographischen Verschlüsselung benutzt werden. Dadurch wird die Sicherung der Übertragung sicherheitsrelevanter Daten zu einem anderen Computersystem, beispielsweise über offene Netzwerke wie dem Internet, gefördert. Insbesondere kann ein stärkeres, vor Angriffen besser geschütztes kryptographisches Verfahren sowie eine größere Schlüssellänge benutzt werden. Durch diese Ausführungsform kann beispielsweise eine gesicherte Authentifikation auf dem anderen Rechnersystem erfolgen, wie es beispielsweise bei der Genehmigung eines Zahlungsvorgangs beim Homebanking erforderlich ist.

Besonders vorzuziehen ist es, wenn zumindest bei der Initialisierung, also dem erstmaligen Aufbau der Datenübertragung zwischen den beiden kommunizierenden Partnern, also beispielsweise zwischen Gateway und Verschlüsselungsclient ein kryptographischer Schlüssel, das anzuwendende kryptographische Verfahren oder beides vereinbart wird. Selbstverständlich kann auch in regelmäßigen Abständen eine neuer Schlüssel ausgehandelt werden, um die Sicherheit weiter zu erhöhen. Dadurch kann bei jeder Datenübertragung ein neuer Schlüssel verwendet werden, so daß Angriffsmöglichkeiten zusätzlich verringert werden. Ferner ist es möglich, die Güte der Verschlüsselung der Vertraulichkeit der zu übertragenden Daten anzupassen. Somit kann beispielsweise für Paßwörter eine hochsichere Datenverbindung geschaffen werden, um maximale Vertraulichkeit der Daten zu gewährleisten, andererseits kann für die Übertragung öffentlicher Daten ein geringerer Sicherheitsstandard gewählt werden, um die Inanspruchnahme der Betriebsmittel des Computersystems zu verringern und somit einen höheren Datendurchsatz zu fördern.

Dabei kann vorteilhafterweise das Verfahren so ausgelegt werden, daß bei Übertragung von nicht sicherheitsrelevanten Daten auf die kryptographische Verschlüsselung der Daten gänzlich verzichtet wird. Eine kryptographische Verschlüsselung erfolgt dann nur noch bei der Übertragung sicherheitsrelevanter Daten, wie beispielsweise Paßwörtern. Somit wird einerseits die nötige Sicherheit, insbesondere Vertraulichkeit, der Datenübertragung, andererseits aber auch größtmöglicher Datendurchsatz der Übertragung bei geringstmöglicher Inanspruchnahme der Betriebsmittel des Computersystems gefördert. Auch können dadurch die für andere, insbesondere bereits vorhandene und nicht auf die Zusammenarbeit mit dem Verschlüsselungsclient angepaßte Anwendungen eingehenden Daten ohne Probleme von diesen anderen Anwendungen empfangen werden.

Bei einer besonders vorzuziehenden Ausführungsweise des erfindungsgemäßen Verfahrens werden die eingehenden Daten, insbesondere die Daten einer Device, mittels vom Betriebssystem zur Verfügung gestellter Zugriffsmöglichkeiten an das verschlüsselnde Mittel übertragen. Dadurch wird es insbesondere vereinfacht, unterschiedlichste Devices verwenden zu können, da die Zugriffsmöglichkeiten des Betriebssystems in der Regel so ausgeführt sind, daß keine Abhängigkeit von der speziellen Ausführungsweise der jeweiligen Device mehr besteht. Beispielsweise stellt das bekannte Betriebssystem WINDOWS® der Firma MICROSOFT® eine solche Zugriffsmöglichkeit in Form von sogenannten "Hook"-Funktionen zur Verfügung. Auch andere Betriebssysteme, wie beispielsweise APPLE-OS® der Firma APPLE® oder UNIX® (z. B. LINUX, Sun Solaris®, Hewlett Packard-UX® usw.) stellen wirkungsähnliche Zugriffsmöglichkeiten zur Verfügung.

Eine besonders vorzuziehende Ausführungsweise des erfindungsgemäßen Verfahrens zeichnet sich dadurch aus, daß überprüft wird, ob auch andere Mittel, insbesondere nicht autorisierte Programme wie Viren oder Trojanische Pferde, auf diese Zugriffsmöglichkeiten des Betriebssystems zugreifen bzw. zuzugreifen beabsichtigen. Dadurch kann ein potentieller Angriff bemerkt werden und Gegenmaßnahmen können eingeleitet werden, wie beispielsweise der Abbruch der Verbindung oder der Versuch, das zuzugreifende Programm zu beenden oder zumindest am Zugriff zu hindern.

Besonders vorzuziehen ist es, wenn eine Meldung generiert wird, und diese beispielsweise in Form einer Warnung an den Benutzer ausgegeben wird, daß die Sicherheit der Datenübertragung nicht mehr gewährleistet ist, so daß dieser geeignete Maßnahmen, wie beispielsweise den Einsatz von Virenscannern oder eine Neuinstallation des Betriebssystems, ergreifen kann.

Eine vorteilhafte Einrichtung zur Durchführung des erfindungsgemäßen Verfahrens weist die Eigenschaft auf, daß sie zumindest ein erstes Mittel aufweist, welches digitale Daten zur Verfügung stellt, sowie ein zweites Mittel aufweist, das die Daten einem kryptographischen Verfahren unterzieht, und diese an andere Mittel des gleichen oder eines anderen Computersystems weitergibt. Dabei ist es gleichgültig, ob das zweite Mittel rein schaltungstechnisch, programmtechnisch oder als Kombination aus beidem, beispielsweise als ein Programm, das auf Funktionen eines kryptographischen Co-Prozessors zugreift, ausgeführt ist. Auch ist es unerheblich, ob das zweite Mittel mit dem ersten Mittel gemeinsam realisiert ist, beispielsweise als externes Gerät, oder ob das zweite Mittel einen Teil der Einrichtung selbst darstellt. Das zweite Mittel sollte möglichst unmittelbar mit dem ersten Mittel zusammenwirken. Andererseits kann es sich als sinnvoll erweisen, andere Mittel zwischen dem ersten und dem zweiten Mittel zuzulassen, um das zweite Mittel möglichst unabhängig von der besonderen Ausführungsform des ersten Mittels ausführen zu können.

Somit weisen die Einrichtungen die oben im Zusammenhang mit den Verfahren beschriebenen Vorteile ebenfalls auf.

Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen.

Im folgen ist ein Ausführungsbeispiel der Erfindung dar-

gestellt, das im weiteren unter Bezugnahme auf die nachfolgend genannten Figuren näher erläutert wird. Dabei werden die Bezeichnungen gemäß der Terminologie des Betriebssystems WINDOWS® der Firma MICROSOFT® verwendet. Ähnliche Vorrichtungen finden sich jedoch auch bei anderen Betriebssystemen, insbesondere bei dem Betriebssystem APPLE-OS® der Firma APPLE® sowie bei dem Betriebssystem UNIX® diverser Hersteller, so daß die Erfindung auch mit solchen Computersystemen realisierbar ist. Es zeigen:

Fig. 1 den prinzipiellen Ablauf eines Verfahrens zur gesicherten Verarbeitung bzw. Übertragung von Daten in schematischer Darstellung;

Fig. 2 eine beispielhafte Ausführung des Verfahrens auf eine Homebanking-Anwendung in schematischer Darstellung;

Fig. 3 ein beispielhaftes Ablaufschema für einen auf der vorliegenden Erfindung basierenden Verschlüsselungsclient;

Fig. 4 ein beispielhaftes Ablaufschema für ein Empfangsmittel (Gateway) der Bank für das Ausführungsbeispiel nach **Fig.** 2.

Fig. 1 zeigt den prinzipiellen Ablauf des Verfahrens auf einer zur Durchführung des Verfahrens geeigneten Einrichtung. Die Daten **11**, die von einer datenliefernden Device (also einer eigenständigen Einheit) **10**, beispielsweise einer Tastatur, herrühren, werden mit Hilfe eines Gerätetreibers (Device Driver) **12** in ein von der Device **10** unabhängiges Datenformat umgewandelt, so daß die Daten **13** nunmehr in einer standardisierten Form vorliegen. Das Format der Daten **13** ist also das gleiche unabhängig davon, ob die Daten beispielsweise von einer Tastatur, einem Fingerabdruckscanner, einem Touchscreen, einem Touchpad, einer Maus, einem Kartelesegerät oder ähnlichem herrühren. Es ist ferner von der jeweiligen konkreten Ausführungsform (Bauart) der Device unabhängig. Die standardisierten Daten **13** werden von einem Verschlüsselungsclient **14** einem kryptographischen Verfahren unterzogen, das erfindungsgemäß beliebig ist. Es kann sich dabei insbesondere um das symmetrische DES®-Verfahren oder dessen Abwandlungen, aber auch um asymmetrische Public-Key-Encryption-Verfahren wie dem RSA®-Verfahren oder dem Diffie-Hellmann-Verfahren mit jeweils beliebiger Schlüssellänge handeln. Der Verschlüsselungsclient **14** kann dabei zusätzliche Aufgaben übernehmen, wie beispielsweise die Überwachung, ob andere, nicht autorisierte Mittel wie beispielsweise Viren oder Trojanische Pferde, die Daten der Device lesen wollen, und nötigenfalls eine Warnmeldung für den Benutzer ausgeben.

Die ursprünglichen Daten liegen nach der Anwendung des kryptographischen Verfahrens in einer kryptographisch verschlüsselten Form **15** vor und können in dieser Form an die jeweilige Anwendung **16**, beispielsweise das bereits erwähnte und im folgenden weiter beschriebene Gateway, welche sich auf dem ursprünglichen Computersystem, einem anderen Computersystem, oder auch auf beiden Computersystemen befindet, weitergegeben werden. Diese Anwendung **16** kann die verschlüsselten Daten nunmehr einem inversen kryptographischen Verfahren unterziehen, um diese weiterzuverarbeiten, oder um diese an andere Anwendungen weiterzureichen. Es ist auch möglich, daß die Anwendung **16** die Daten **15** nochmals einem kryptographischen Verfahren unterzieht, wobei dieses Verfahren so gewählt werden kann, daß dieses höheren Sicherheitsanforderungen genügt, und erst dann über ein Netzwerk an einen anderen Rechner übermittelt.

In jedem Fall liegen die Daten im Client-Computer **110** (**Fig.** 2) in kryptographisch verschlüsselter Form vor, so daß insbesondere Angriffe auf die Vertraulichkeit der Daten durch unbefugte Mittel, wie beispielsweise Viren oder Trojanische Pferde, deutlich erschwert werden.

Es ist ebenso denkbar, den Verschlüsselungsclient **14** bereits auf die ursprünglich von der Device gelieferten Daten **11** anzuwenden. Da diese Daten jedoch in einem Format vorliegen, welches von der jeweiligen Device abhängig ist, ist bei diesem Vorgehen eine Anpassung des Verschlüsselungsclients **14** auf die jeweilige Device **10** erforderlich, was einen entsprechenden Aufwand erforderlich macht. Der Vorteil bei diesem Verfahren liegt in einer gegenüber dem vorherigen Verfahren, bei dem erst die Daten **13**, die von einem Gerätetreiber **12** geliefert werden, dem kryptographischen Verfahren unterzogen werden, nochmals erhöhter Sicherheit.

Fig. 2 zeigt die beispielhafte Anwendung des Verfahrens auf eine Homebanking-Anwendung in schematischer Darstellung. Dabei befindet sich der Benutzer an einem Client-Computer **110** und gibt an diesem Daten über ein entsprechendes Eingabegerät (Device) **120**, hier eine Tastatur, ein. Über ein Netzwerk **101**, wobei es sich um ein Local Area Network (LAN, ein lokales Netzwerk), ein Wide Area Network (WAN, ein globales Netzwerk) oder eine Kombination aus beidem handeln kann, gelangen die Daten zu einen Server-Computer **100**, welcher sich beispielsweise bei der Bank befindet. In dem dargestellten Ausführungsbeispiel fordert der Benutzer mit einem WWW-Browser **140** (beispielsweise dem "Netscape Navigator®" oder dem "Internet Explorer®") eine WWW-Seite an, die eine entsprechende Eingabemaske für das Homebanking zur Verfügung stellt. Diese WWW-Seite startet zusätzlich ein Programm zur Initialisierung und Durchführung des gesicherten Datenverarbeitungs- und Übertragungsverfahrens. Im dargestellten Ausführungsbeispiel wird ein Java®-Applet mit einer Java®-Bean **143** (also ein Programmteil, das unmittelbar nach dem Laden ausgeführt wird) geladen, wodurch das Java®-Bean **143** initialisiert wird. Das Java®-Bean **143** ruft wiederum das hier auf dem Server-Computer **100** (der nicht unbedingt mit dem Server, der die WWW-Seite zur Verfügung stellt übereinstimmen muß) ausgeführte Gateway **130** auf. Dabei kommuniziert das Java®-Bean **143** mit dem Gateway **130** mittels einer Datenübertragung **115**, **116**, über das Netzwerk **101**, wobei der Datenfluß **115** vom Java®-Bean **143** zum Gateway **130** über den Socket-Server des Java®-Beans **141** zum Socket-Client des Gateways **132** erfolgt, der Datenfluß **116** vom Gateway **130** zum Java®-Bean **143** dagegen über den Socket-Server des Gateways **131** zum Socket-Client des Java®-Beans **142** erfolgt.

Das Gateway erzeugt (generiert) nun einen Schlüssel, welcher zur Durchführung des anschließend verwendeten kryptographischen Verfahrens benutzt wird.

Anschließend ruft das Gateway **130** den Verschlüsselungsclient **125** auf. Die Kommunikation zwischen Gateway **130** und Verschlüsselungsclient **125** erfolgt dabei unter Benutzung des Netzwerks **101** über den Datenstrom **117** vom Socket-Server des Verschlüsselungsclients **121** hin zum Socket-Client des Gateways **132** sowie über den Datenstrom **118** vom Socket-Server des Gateways **131** hin zum Socket-Client des Verschlüsselungsclients **122**.

Über die Datenverbindung **117**, **118** handeln Gateway **130** und Verschlüsselungsclient **125** den kryptographischen Schlüssel aus, wodurch der Verschlüsselungsclient **125** auf sicherem Wege einen Schlüssel erhält. Das verwendete kryptographische Verfahren sowie die Schlüssellänge sind dabei beliebig.

Eine direkte Kommunikation des Java®-Beans **143** mit der Hook-Funktion **126**, die vom Betriebssystem zur Verfügung gestellt wird, oder mit dem Verschlüsselungsclient **125** ist nicht möglich, da das Sicherheitskonzept der Programmiersprache Java® eine solche Kommunikation nicht zuläßt.

Aus diesem Grund erfolgt die Kommunikation des Java®-Beans **143** mit der Hook-Funktion **126** über das das Java®-Bean **143** initialisierende Gateway **130** auf dem Server-Computer **100**, von diesem aus zu einem entsprechend ausgeführten Verschlüsselungsclient **125** auf dem Client-Computer **110**, der widerum auf die Hook-Funktion **126** zuzugreifen vermag.

Sobald die Initialisierung des Verschlüsselungsclient **125** abgeschlossen ist, sendet dieser eine "Bereit"-Meldung an das Gateway **130**, welches wiederum die "Bereit"-Meldung an das Java®-Bean **143** weitergibt.

Sobald nun bei der im WWW-Browser **140** dargestellten Eingabemaske ein Feld aktiviert wird, welches eine vertraulich zu behandelnde Eingabe erfordert, hier ein Paßwort, wird ein "Focus"-Status auf den Wert "Verschlüsseln" gesetzt. Dieser "Focus"-Status wird dem Verschlüsselungsclient **125** vom Java®-Bean **143** über das Gateway **130** gemeldet, woraufhin dieses von der Tastatur **120** eingehende Daten **127** unmittelbar nach dem Gerätetreiber (Device-Driver) **123** mit Hilfe der "Hook"-Funktion **126** abfängt und dem vereinbarten kryptographischen Verfahren unterzieht. Die an das Gateway **130** weitergeleiteten Daten **117** sind damit verschlüsselt. Dabei ist die "Hook"-Funktion **126** eine vom Betriebssystem, in diesem Fall WINDOWS® der Firma MICROSOFT®, zur Verfügung gestellte Funktion. Die verschlüsselten Daten **117** werden vom hier auf dem Server-Computer **100** befindlichen Gateway **130** beim hier dargestellten Ausführungsbeispiel entschlüsselt und anderen, hier nicht dargestellten Anwendungen zur Verfügung gestellt. Zusätzlich sendet der Socket-Server des Gateways **131** über den Datenstrom **116** für jede gedrückte Taste der Tastatur **120** ein beliebiges Zeichen an den Socket-Client des Java®-Beans **142**. Dieses stellt, unabhängig vom empfangenen Zeichen, ein beliebiges Zeichen, hier einen Stern, in dem Datenfeld für das einzugebende Paßwort dar, um so eine Rückkopplung an den Benutzer zu bewirken.

Sobald der Benutzer des Client-Computers **110** ein anderes Datenfeld aufruft, oder die Eingabemaske des WWW-Browsers **140** verläßt, sendet das Java®-Bean **143** über das Gateway **130** den "Focus"-Status "Unverschlüsselt" an den Verschlüsselungsclient **125**.

Daraufhin schickt der Verschlüsselungsclient **125** eine "Bereit"-Meldung an das Gateway **130**, welches die "Bereit"-Meldung an das Java®-Bean **143** weitergibt, und gibt daraufhin die Daten der Tastatur **120** unverschlüsselt weiter, wendet also das kryptographische Verfahren nicht mehr auf die Daten an.

Es wäre auch denkbar, das Gateway **130** auf dem Client-Computer **110** auszuführen, um dort eine Authentifizierung des Benutzers durchzuführen. Auch wäre es möglich ein zusätzliches, hier nicht dargestelltes Mittel auf dem Client-Computer **110** vorzusehen, das auf die von der Tastatur **120** an den Server-Computer **100** gesendeten Daten **117** ein zusätzliches, insbesondere ein besonders sicheres, Verschlüsselungsverfahren anwendet.

In **Fig. 3** ist beispielhaft ein Ablaufschema für den Verschlüsselungsclient **125** dargestellt. Eine Tastatureingabe **127, 200** wird im dargestellten Ausführungsbeispiel vom Verschlüsselungsclient **125** über die "Hook"-Funktion **126**, welche vom Betriebssystem bereitgestellt ist, unmittelbar nach Durchlaufen des Gerätetreibers (Device-Driver) **123** empfangen. Der Verschlüsselungsclient prüft anhand des bereits beschriebenen "Focus"-Status, ob eine gesicherte Eingabe erforderlich ist 201.

Ist der "Focus"-Status "Unverschlüsselt" gesetzt, also eine gesicherte Eingabe nicht erforderlich 205, so erfolgt eine unverschlüsselte Standardübergabe der Daten an andere Anwendungen **206** des Server-Computers **100** und/oder Client-Computers **110**, also so, als ob der Verschlüsselungsclient **125** nicht vorhanden wäre. Somit können insbesondere bereits vorhandene, nicht auf die Zusammenarbeit mit dem Verschlüsselungsclient eingerichtete Anwendungen problemlos weiterverwendet werden.

Ist dagegen der "Focus"-Status "Verschlüsseln" gesetzt, so ist eine gesicherte Eingabe erforderlich 210. Es erfolgt eine Prüfung **211**, ob ein weiteres Mittel auf die "Hook"-Funktion zugreift, also ob ein anderes, nicht autorisiertes Mittel wie beispielsweise ein Virus oder ein Trojanisches Pferd die Tastatureingabe abzufragen versucht.

Ergibt die Prüfung, daß ein weiteres Mittel auf die "Hook"-Funktion zugreift 220, so wird versucht, das weitere Mittel zu beenden 221.

Sofern der Versuch, das weitere Mittel zu beenden, nicht erfolgreich ist 225, so ist die Sicherheit, insbesondere die Vertraulichkeit der eingegebenen Daten nicht mehr gewährleistet. Die Tastatureingabe kann wahlweise mit oder ohne Verschlüsselung weitergeleitet werden 226. In jedem Fall erfolgt zusätzlich eine Warnung **227** an den Benutzer, daß die Datensicherheit potentiell nicht gewährleistet ist. Vorteilhafterweise wird die Tastatureingabe jedoch mit Verschlüsselung weitergeleitet, da die Daten dann zumindest während der Übertragung über das Netzwerk **101** geschützt sind.

Ist dagegen das Beenden des weiteren Mittels erfolgreich 222, wird die Eingabe in der Folge verschlüsselt 216, so als ob von vornherein die Abfrage **211**, ob ein weiteres Mittel auf die "Hook"-Funktion zugreift, ergeben hätte, daß kein weiteres Mittel auf die "Hook"-Funktion zugreift 215.

Sofern eine Verschlüsselung der eingegebenen Daten **216** erfolgen soll, wird sicherheitshalber überprüft, ob die Verschlüsselung der Tastatureingabe tatsächlich erfolgreich ist.

Ist die Verschlüsselung nicht erfolgreich 230, erfolgt eine Weiterleitung der Tastatureingabe ohne Verschlüsselung **231** an die jeweilige Anwendung und gleichzeitig erfolgt eine Warnmeldung **232** an den Benutzer, daß die Sicherheit der Tastatureingabe **200** nicht gewährleistet ist.

Verläuft die Verschlüsselung dagegen erfolgreich 235, so werden die Daten in verschlüsselter Form an die jeweilige Anwendung übergeben 236.

Verläuft auch die Übergabe erfolgreich 240, so ist der Verschlüsselungsprozeß standardmäßig abgeschlossen 241 und die Daten liegen in verschlüsselter Form bei der jeweiligen Anwendung vor, beispielsweise beim bereits beschriebenen Gateway **130**.

Verläuft die Übergabe der Daten an die jeweilige Anwendung **236** dagegen nicht erfolgreich 245, so wird die Verschlüsselungsfunktion beendet 246. Es kann somit eine erneute Tastatureingabe **247** erfolgen, bei der die Daten nunmehr an die jeweilige Anwendung weitergeleitet werden, wenn auch in unverschlüsselter Form. Zusätzlich erfolgt wiederum eine Warnmeldung **248** an den Benutzer, daß die Sicherheit der Tastatureingabe **200** nicht gewährleistet ist.

In **Fig. 4** ist schließlich für das dargestellte Ausführungsbeispiel einer Homebanking-Anwendung, welches auf der vorliegenden Erfindung basiert, das an sich bekannte Empfangs- und Entschlüsselungsverfahren durch das Gateway **130** des Server-Computers **100** bei der Bank schematisch dargestellt. Die über das Netzwerk **101** am Dateneingang **300** eingehenden Daten **102** werden zunächst daraufhin geprüft, ob diese insbesondere durch einen Verschlüsselungsclient durch Anwendung eines kryptographischen Verfahrens gesichert sind 301.

Liegen die Daten in unverschlüsselter Form **305** vor, so werden diese direkt an die Zielanwendung (Zielapplikation) weitergegeben 315.

Liegen die Daten dagegen in verschlüsselter Form vor

310, wurden also diese vom Verschlüsselungsclient **125** erfolgreich in verschlüsselter Form übergeben 240, so wird zunächst ein Mittel zur Entschlüsselung der verschlüsselten Daten aufgerufen 311, welches ein entsprechendes inverses kryptographisches Verfahren auf die eingegangenen Daten anwendet 312. Die dann in ihrer ursprünglichen Form vorliegenden Daten werden schließlich an die Zielanwendung (Zielapplikation) weitergegeben 315.

Patentansprüche

1. Verfahren zur gesicherten Verarbeitung und/oder Übertragung von digitalen Daten, insbesondere bei vernetzten Computersystemen, **dadurch gekennzeichnet**, daß in zumindest ein Computersystem eingehende Daten vor der Weiterbenutzung innerhalb des Computersystems einem kryptographischen Verfahren unterzogen werden.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Daten zumindest einer Device von einem als Verschlüsselungsclient wirkenden Mittel dem kryptographischen Verfahren unterzogen werden.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Daten einer Eingabeeinrichtung, insbesondere einer Tastatureinrichtung, von einem als Verschlüsselungsclient wirkenden Mittel dem kryptographischen Verfahren unterzogen werden.
4. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Daten von zumindest einem als Gateway wirkenden Mittel eines der beteiligten Computersysteme empfangen werden und von diesem einem inversen kryptographischen Verfahren unterzogen werden.
5. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Daten vor der Übertragung zu einem zweiten Computersystem von einem zusätzlichen Verschlüsselungsmittel des ersten Computersystems einem weiteren kryptographischen Verfahren unterzogen werden.
6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß zumindest bei der Initialisierung der Datenübertragung ein Schlüssel und/oder das anzuwendende kryptographische Verfahren, insbesondere zwischen Verschlüsselungsclient und dem Gateway, zwischen Verschlüsselungsclient und einem zusätzlichem Verschlüsselungsmittel und/oder zwischen zusätzlichem Verschlüsselungsmittel und Gateway vereinbart wird.
7. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß das kryptographische Verfahren nur bei der Übertragung bestimmter, insbesondere sicherheitsrelevanter Daten angewandt wird.
8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß die eingehenden Daten mittels vom Betriebssystem zur Verfügung gestellter Zugriffsmöglichkeiten an das als Verschlüsselungsclient wirkende verschlüsselnde Mittel übertragen werden.
9. Verfahren nach einem der vorangehenden Ansprüche, insbesondere nach Anspruch 8, dadurch gekennzeichnet, daß überprüft wird, ob ein anderes Mittel, insbesondere ein nicht autorisiertes Programm, auf die vom Betriebssystem zur Verfügung gestellte Zugriffsmöglichkeit zugreift beziehungsweise zuzugreifen beabsichtigt.
10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, daß eine Meldung generiert wird, wenn ein anderes Mittel auf die vom Betriebssystem zur Verfügung gestellte Zugriffsmöglichkeit zugreift beziehungsweise zuzugreifen beabsichtigt.
11. Einrichtung mit mindestens einer Recheneinheit, die derart eingerichtet ist, daß das Verfahren nach einem der Ansprüche 1 bis 10 durchführbar ist.
12. Einrichtung zur gesicherten Verarbeitung und/oder Übertragung von digitalen Daten, insbesondere bei vernetzten Computersystemen, das mindestens folgende Mittel umfaßt:
ein erstes Mittel, das digitale Daten zur Verfügung stellt,
ein zweites Mittel, das die Daten einem kryptographischen Verfahren unterzieht, und an andere Mittel übermittelt.
13. Einrichtung nach Anspruch 12, dadurch gekennzeichnet, daß zumindest eine Device als erstes Mittel vorgesehen ist.
14. Einrichtung nach Anspruch 12 oder 13, dadurch gekennzeichnet, daß eine Eingabeeinrichtung, insbesondere eine Tastatureinrichtung als erstes Mittel vorgesehen ist.
15. Einrichtung nach einem der Ansprüche 12 bis 14, dadurch gekennzeichnet, daß zumindest ein drittes Mittel vorgesehen ist, das die Daten des zweiten Mittels einem inversen kryptographischen Verfahren unterzieht.
16. Einrichtung nach einem der Ansprüche 12 bis 15, dadurch gekennzeichnet, daß zumindest ein viertes Mittel vorgesehen ist, das die Daten des zweiten und/oder dritten Mittels einem weiteren kryptographischen Verfahren unerzieht.
17. Einrichtung nach einem der Ansprüche 12 bis 16, dadurch gekennzeichnet, daß das zweite und/oder dritte und/oder vierte Mittel so ausgeführt sind, daß zumindest bei Initialisierung der Datenübertragung zwischen dem zweitem Mittel und dem drittem Mittel oder einem zweiten Computersystem, beziehungsweise dem vierten Mittel und dem zweiten Computersystem ein Schlüssel und/oder das anzuwendende kryptographische Verfahren vereinbart wird.
18. Einrichtung nach einem der Ansprüche 12 bis 17, dadurch gekennzeichnet, daß das zweite und/oder dritte und/oder vierte Mittel so ausgeführt ist, daß das kryptographische Verfahren nur bei der Übertragung bestimmter, insbesondere sicherheitsrelevanter Daten angewandt wird.
19. Einrichtung nach einem der Ansprüche 12 bis 18, insbesondere nach Anspruch 18, dadurch gekennzeichnet, daß das zweite Mittel so ausgeführt ist, daß es mit geeigneten, vom Betriebssystem der Einrichtung zur Verfügung gestellten Zugriffsmöglichkeiten zusammenwirkt.
20. Einrichtung nach einem der Ansprüche 12 bis 19, dadurch gekennzeichnet, daß das zweite Mittel so ausgeführt ist, daß es erkennt, wenn andere Mittel, insbesondere nichtautorisierte Programme, auf die Zugriffsmöglichkeiten des Betriebssystems der Einrichtung zugreifen beziehungsweise zuzugreifen beabsichtigen.
21. Einrichtung nach Anspruch 19, dadurch gekennzeichnet, daß das zweite Mittel so ausgeführt ist, daß es eine Warnung ausgibt, wenn es erkennt, daß andere Mittel auf die Zugriffsmöglichkeiten des Betriebssystems der Einrichtung zugreifen beziehungsweise zuzugreifen beabsichtigen.
22. Computerprogrammprodukt, das direkt in den internen Speicher eines digitalen Computers geladen werden kann und Softwarecodeabschnitte umfaßt, mit denen die Schritte gemäß einem der Ansprüche 1 bis 10

ausgeführt werden, wenn das Produkt auf einem Computer läuft.

23. Computerprogrammprodukt, das auf einem computergeeigneten Medium gespeichert ist und computerlesbare Programmittel gemäß einem der Ansprüche 11 bis 21 umfaßt.

Hierzu 4 Seite(n) Zeichnungen

Nummer: DE 100 06 062 A1
Int. Cl.[7]: H 04 L 9/00
Offenlegungstag: 30. August 2001

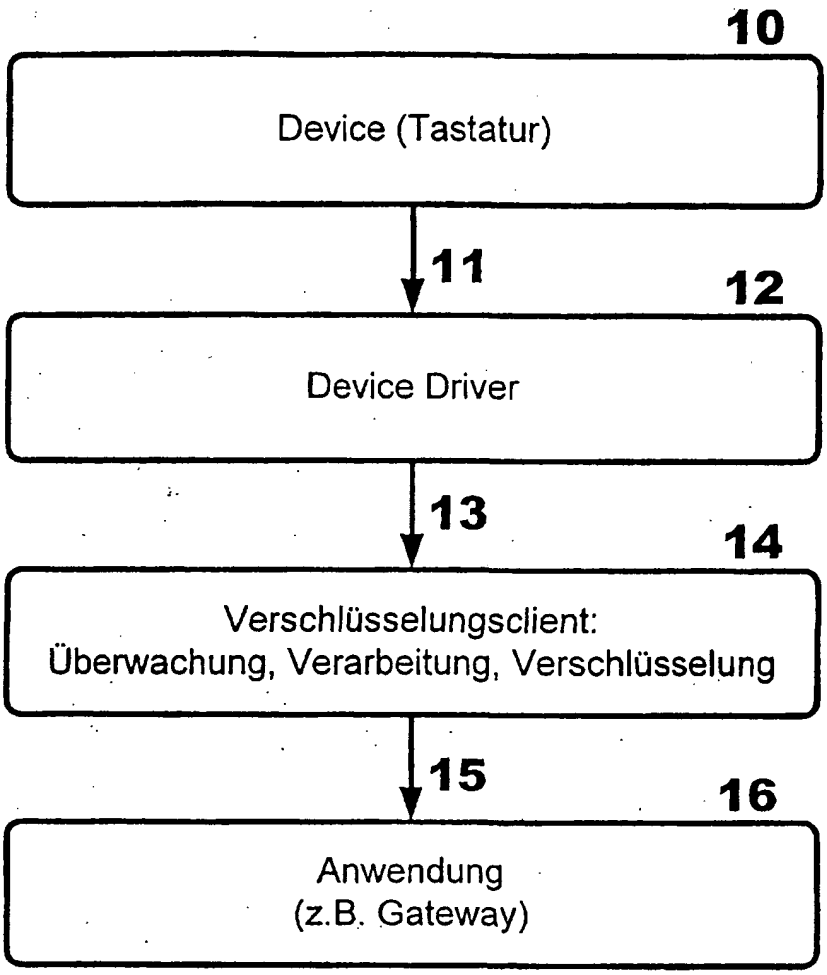

Fig. 1

Nummer: DE 100 06 062 A1
Int. Cl.[7]: H 04 L 9/00
Offenlegungstag: 30. August 2001

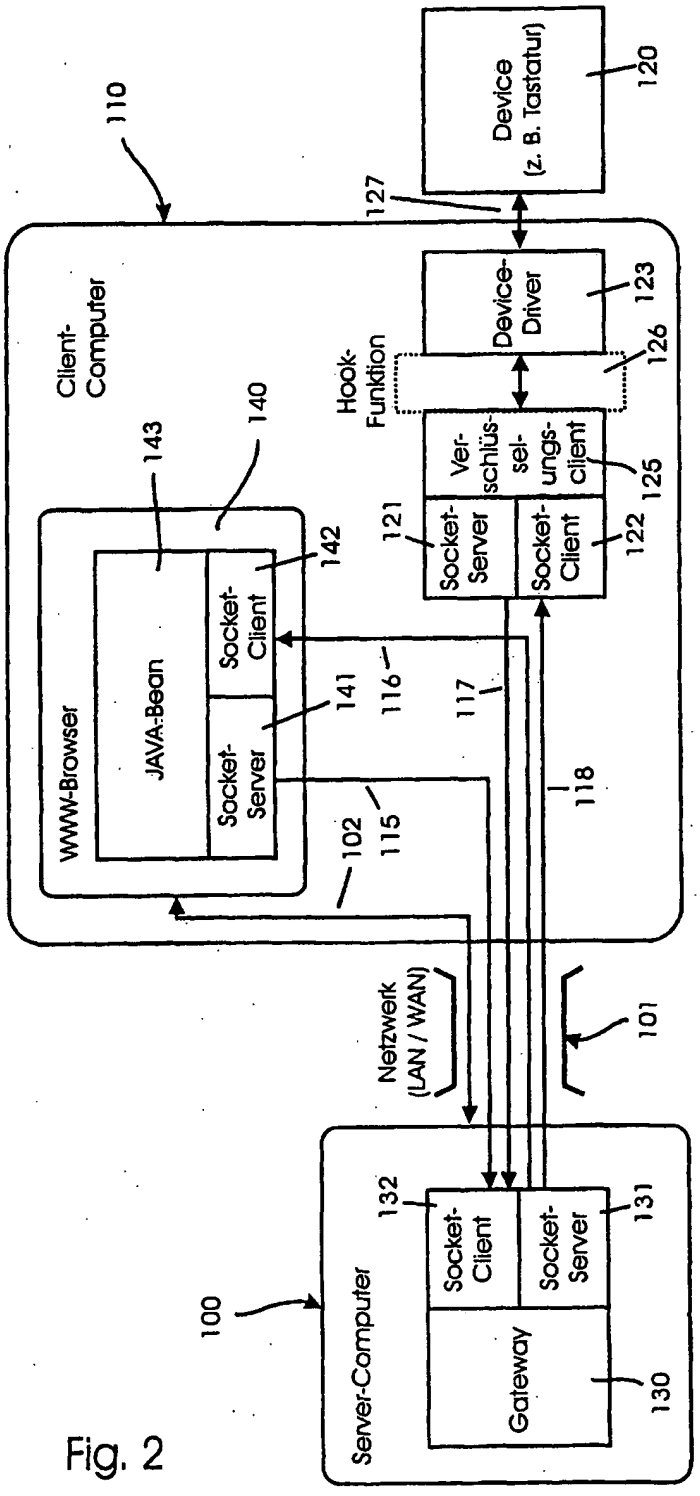

Fig. 2

Nummer: DE 100 06 062 A1
Int. Cl.[7]: H 04 L 9/00
Offenlegungstag: 30. August 2001

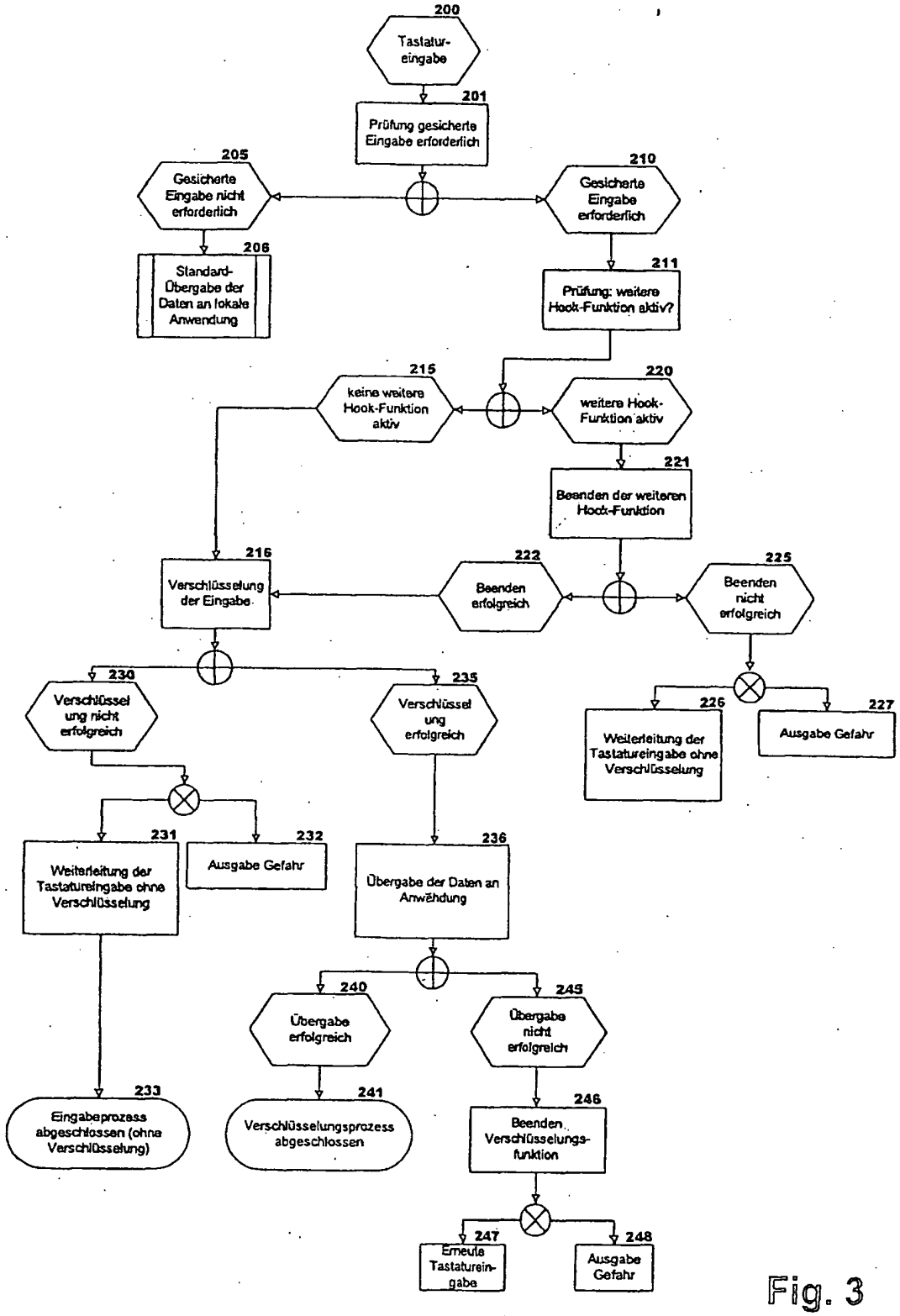

Fig. 3